REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Amendments to the Claims

Claim 1 is amended replacing the expression "prime number" with "order" on lines 5 and 6.

Claim 5 is amended inserting "a" between "is" and "prime" on line 1.

Claim 9 is amended inserting "said" between "than" and "order" on lines 9 and 10.

Claim Rejections – 35 U.S.C. § 112

Claim 1 has been rejected under 35 U.S.C. § 112, second paragraph as being indefinite due to an alleged lack of antecedence for the expression "said prime number q". Applicant amends claim 1 replacing "said prime number q" with "said order q". The expression "order q" is introduced in the preamble of claim 1. Therefore, Applicant believes that claim 1 as amended complies with 35 U.S.C. § 112, second paragraph.

Claim Rejections – 35 U.S.C. § 103

Regarding Claims 1-2, 4-5:

Claims 1-2, and 4-5 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier (pages 483-490) in view of US Patent No. 6,307,938 to Matyas Jr. et al. (hereinafter Matyas). Applicant respectfully traverses the rejections as follows.

Schneier teaches the digital signature algorithm (DSA) proposed for use in the Digital Signature Standard (DSS) by the National Institute of Standards and Technology (NIST). The Examiner relies primarily on page 487, line 11, where Alice generates a random number k which is less than q. Based on this step, the Examiner believes that Schneier teaches the step of generating a seed value from a random number (i.e. k), and the steps of accepting or rejecting the output based on whether or not it is less than a prime q. Applicant acknowledges that the Examiner admits that Schneier does not teach comparing a hashed version of a seed value with a value q. The Examiner relies on Matyas as teaching what is missing from Schneier, specifically, the passage from column 6, line 65 to column 8, line 35.

In the above-noted passage, Matyas outlines the ANSI X9.31 method of prime number

generation involving hashing SEED values to generate the needed random numbers for generating the primes p and q. Assuming one SEED, the method proceeds to choose a SEED, hash the SEED, generate a random number (RN) from the hashed SEED, generate a prime (p) from the RN, and perform a primality test on the prime p. In practice, several SEED values are used to generate the RN and prime p. The prime p is chosen from an iterative process that applies the primality test to the value chosen for p until certain criteria are met.

Applicant respectfully submits that:

1) Matyas does not teach performing a hash as asserted by the Examiner, let alone as recited in claim 1; and
2) Even if for the sake of argument Matyas did teach performing a hash as the Examiner asserts, there is no motivation to combine Matyas with Schneier.

Regarding 1), as noted above, the ANSI X9.31 procedure generates a prime from random numbers derived from the hash of a SEED value. However, there is no step of comparing an output (let alone an output destined to be a key) with an established value of order q to determine if that output is less than the prime, as the Examiner asserts. It is the Applicant's recognition that by choosing the key as recited in claim 1, the bias in the selection of k (identified by the work of Daniel Bleichenbacher) can be minimized.

The ANSI X9.31 method taught by Matyas does not recognize this bias nor provide any steps to avoid the bias, let alone hash a seed value and use this hashed value as an output to determine if the output is less than a predetermined value of a certain order as claimed. In fact, the ANSI method taught by Matyas teaches generating a random number from a hashed SEED, whereas claim 1 recites generating a seed from a random number and then hashing the seed value to produce an output. Therefore the teachings of Matyas relied upon by the Examiner are quite contrary to what is recited in claim 1.

According to MPEP 2143, one of the criteria for establishing a *prima facie* case of obviousness is that the relied upon references teach every element in the claim. Clearly, neither Schneier nor Matyas teach performing a hash function on a seed value that is chosen from a random number generator as recited in claim 1. In fact, the teachings of Matyas that are relied upon by the Examiner teach performing a hash on a seed first and then generating a random number from the hash value, which is quite contrary to what is claimed.

Regarding 2), Schneier teaches in the realm of digital signatures, wherein a number q is

used in generating signature components *r* and *s*, whereas Matyas teaches in the realm of generating prime numbers from a series of seed values. Clearly there is no direction in the teachings of Schneier to look to the teachings of Matyas since they teach entirely different schemes for achieving entirely different results. In fact, there is nothing in either Schneier or Matyas that would encourage a person skilled in the art to combine the teachings. The Examiner relies on column 7, lines 5-6 from Matyas as providing the motivation to combine the references. In this passage Matyas merely states that it is not possible to invert the hash to determine the required input SEED(s). Applicant believes that this does not provide sufficient motivation since the mere acknowledgement that a hash function is theoretically irreversible does not teach how to implement the hash in generating a key as recited in claim 1. There is simply no suggestion or motivation to make such a leap of logic.

Applicants respectfully submit that not only do Schneier and Matyas, either in combination or alone, fail to teach every element recited in claim 1, but there is no suggestion or motivation to even make such a combination. Therefore, Applicants believe that claim 1 clearly and patentably distinguishes over the combination of Schneier in view of Matyas and as such is in condition for allowance.

Claims 2 and 4-5 being ultimately dependent on claim 1 are also believed to distinguish over the prior art cited.

Regarding Claims 7-13:

Claims 7-13 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Backal. Applicant respectfully traverses the rejections as follows.

Backal teaches a virtual key method using a virtual matrix to avoid sending large keys over a communication channel. Claims 7-8 are ultimately dependent on claim 1, which Applicant submits, distinguishes over Schneier in view of Matyas. Therefore, Backal must not only teach the subject matter of claims 7-8 but also what is missing from Schneier and Matyas. Backal does not teach determining whether an output is less than a number of order *q*, where the output is provided by performing a hash function on a seed number generated from a random number generator. Therefore, Backal at least fails to teach what is missing from Schneier and Matyas, and as such, claims 7-8 are believed to distinguish over the Schneier in view of Matyas,

in further view of Backal, for at least that reason.

Claim 9 is an independent claim that, similar to claim 1, determines whether an output is less than a number of order *q*, where the output is provided in part by performing a hash function on a seed number generated from a random number generator. Therefore, arguments made regarding claim 1 over Schneier and Matyas equally apply to claim 9. As noted above, Backal does not teach what is missing from Schneier and Matyas. Therefore, claim 9 is believed to patentably distinguish over Schneier, in view of Matyas, in further view of Backal for at least that reason.

Claims 10-13 being ultimately dependent on claim 9 are also believed to distinguish over the prior art cited.

Regarding Claims 3 and 6:

Claims 3 and 6 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Nel. Applicant respectfully traverses the rejections as follows.

Nel teaches key generation for the DSS, specifically, a summary of the private key generation method found in the original draft DSA proposal by NIST. Claims 3 and 6 are ultimately dependent on claim 1, which Applicant submits, distinguishes over Schneier in view of Matyas. Therefore, Nel must not only teach the subject matter of claims 3 and 6 but also what is missing from Schneier and Matyas. Nel does not teach determining whether an output is less than a number of order *q*, where the output is provided by performing a hash function on a seed number generated from a random number generator. Therefore, Nel at least fails to teach what is missing from Schneier and Matyas, and as such, claims 3 and 6 are believed to distinguish over the Schneier in view of Matyas, in further view of Nel, for at least that reason.

Regarding Claim 14:

Claim 14 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Backal, in further view of Nel. Applicant respectfully traverses the rejections as follows. Applicant notes that the Examiner also mentions Matyas in this rejection. Applicant assumes that the Examiner intended to include Matayas, and thus claim 14 is assumed to have been rejected over Schneier, in view of Matyas, in further view of Backal, in further view of Nel.

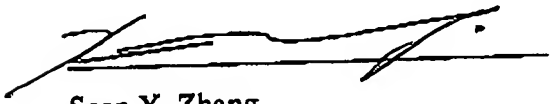
Claim 14 is ultimately dependent on claim 9, which Applicant submits, distinguishes over Schneier in view of Matyas, in further view of Backal. Therefore, Nel must not only teach the subject matter of claim 14 but also what is missing from Schneier, Matyas, and Backal. As noted above, Nel does not teach determining whether an output is less than a number of order q, where the output is provided by performing a hash function on a seed number generated from a random number generator. Therefore, Nel at least fails to teach what is missing from Schneier, Matyas, and Backal, and as such, claim 14 is believed to distinguish over Schneier, in view of Matyas, in further view of Backal, in further view of Nel, for at least that reason.

Summary

In view of the foregoing, Applicant respectfully submits that all pending claims, namely claims 1-14 patentably distinguish over the prior art cited by the Examiner, and as such are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Sean X. Zhang
Agent for Applicant
Registration No. 56,058

Date: March 3, 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.5839
SZH/BSL